Listing and Amendments to the Claims

1. (currently amended) Method for encrypting data ~~renewing a symmetric key~~ in a communication network comprising a device of a first type containing:

- a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network, wherein said second type of device is a different device type from said device of a first type; and

- and an encrypted first symmetric key which is generated from the encryption of said first symmetric key ~~encrypted~~ with a second symmetric network key known only by at least one device of a second type connected to said network;

the method comprising the steps ~~that consist,~~ for the device of a first type of~~, in~~:

(a) generating a random number;

(b) computing a new symmetric key as a function of the first symmetric key and said random number;

(c) encrypting the data to be transmitted with the new symmetric key; and

(d) transmitting to a device of a second type, via said network:

- the data encrypted with the new symmetric key;
- the random number; and
- said encrypted first symmetric key. ~~encrypted with the second symmetric network key.~~

2. (currently amended) Method according to claim 1, wherein the function used to compute the new symmetric key is a one-way derivation function.

3. (currently amended) Method according to claim 2, wherein the function is a hash ~~or encryption~~ function.

4. (currently amended) Method according to claim 1, also comprising the steps ~~consisting,~~ for the device of a second type that receives data transmitted at step (d) of ~~, in~~:

(e) decrypting, with the second symmetric network key the encrypted first symmetric key as to produce ~~encryption of~~ the first symmetric key;

(f) determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key; and

(g) decrypting the data received with the new symmetric key ~~thus obtained~~.